Subpart C—Vessel Security Assessment (VSA)

§ 104.300 General.

(a) The Vessel Security Assessment (VSA) is a written document that is based on the collection of background information and the completion and analysis of an on-scene survey.

(b) A single VSA may be performed and applied to more than one vessel to the extent that they share physical characteristics and operations.

(c) Third parties may be used in any aspect of the VSA if they have the appropriate skills and if the Company Security Officer (CSO) reviews and accepts their work.

(d) Those involved in a VSA should be able to draw upon expert assistance in the following areas:

(1) Knowledge of current security threats and patterns;

(2) Recognition and detection of dangerous substances and devices;

(3) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(4) Techniques used to circumvent security measures;

(5) Methods used to cause a security incident;

(6) Effects of dangerous substances and devices on vessel structures and equipment;

(7) Vessel security requirements;

(8) Vessel-to-vessel and vessel-to-facility interface business practices;

(9) Contingency planning, emergency preparedness and response;

(10) Physical security requirements;

(11) Radio and telecommunications systems, including computer systems and networks;

(12) Marine engineering; and

(13) Vessel and port operations.

§ 104.305 Vessel Security Assessment (VSA) requirements.

(a) *Background.* The vessel owner or operator must ensure that the following background information is provided to the person or persons who will conduct the on-scene survey and assessment:

(1) General layout of the vessel, including the location of:

(i) Each actual or potential point of access to the vessel and its function;

(ii) Spaces that should have restricted access;

(iii) Essential maintenance equipment;

(iv) Cargo spaces and storage;

(v) Storage of unaccompanied baggage; and

(vi) Vessel stores;

(2) Threat assessments, including the purpose and methodology of the assessment, for the area or areas in which the vessel operates or at which passengers embark or disembark;

(3) The previous VSA, if any;

(4) Emergency and stand-by equipment available to maintain essential services;

(5) Number of vessel personnel and any existing security duties to which they are assigned;

(6) Existing personnel training requirement practices of the vessel;

(7) Existing security and safety equipment for the protection of personnel, visitors, passengers, and vessels personnel;

(8) Escape and evacuation routes and assembly stations that have to be maintained to ensure the orderly and safe emergency evacuation of the vessel;

(9) Existing agreements with private security companies providing waterside or vessel security services; and

(10) Existing security measures and procedures, including:

(i) Inspection and control procedures;

(ii) Identification systems;

(iii) Surveillance and monitoring equipment;

(iv) Personnel identification documents;

(v) Communication systems;

(vi) Alarms;

(vii) Lighting;

(viii) Access control systems; and

(ix) Other security systems.

(b) *On-scene survey.* The vessel owner or operator must ensure that an on-scene survey of each vessel is conducted. The on-scene survey is to verify or collect information required in paragraph (a) of this section. It consists of an actual survey that examines and evaluates existing vessel protective measures, procedures, and operations for:

(1) Ensuring performance of all security duties;

(2) Controlling access to the vessel, through the use of identification systems or otherwise;

(3) Controlling the embarkation of vessel personnel and other persons and their effects, including personal effects and baggage whether accompanied or unaccompanied;

(4) Supervising the handling of cargo and the delivery of vessel stores;

(5) Monitoring restricted areas to ensure that only authorized persons have access;

(6) Monitoring deck areas and areas surrounding the vessel; and

(7) The ready availability of security communications, information, and equipment.

(c) *Analysis and recommendations.* In conducting the VSA, the Company Security Officer (CSO) must analyze the vessel background information and the on-scene survey, and while considering the requirements of this part, provide recommendations for the security measures the vessel should include in the Vessel Security Plan (VSP). This includes but is not limited to the following:

(1) Restricted areas;

(2) Response procedures for fire or other emergency conditions;

(3) Security supervision of vessel personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.;

(4) Frequency and effectiveness of security patrols;

(5) Access control systems, including identification systems;

(6) Security communication systems and procedures;

(7) Security doors, barriers, and lighting;

(8) Any security and surveillance equipment and systems;

(9) Possible security threats, including but not limited to:

(i) Damage to or destruction of the vessel or an interfacing facility or vessel by dangerous substances and devices, arson, sabotage, or vandalism;

(ii) Hijacking or seizure of the vessel or of persons on board;

(iii) Tampering with cargo, essential vessel equipment or systems, or vessel stores;

(iv) Unauthorized access or use, including presence of stowaways;

(v) Smuggling dangerous substances and devices;

(vi) Use of the vessel to carry those intending to cause a security incident and/or their equipment;

(vii) Use of the vessel itself as a weapon or as a means to cause damage or destruction;

(viii) Attacks from seaward while at berth or at anchor; and

(ix) Attacks while at sea; and

(10) Evaluating the potential of each identified point of access, including open weather decks, for use by individuals who might seek to breach security, whether or not those individuals legitimately have access to the vessel.

(d) *VSA report.* (1) The vessel owner or operator must ensure that a written VSA report is prepared and included as part of the VSP. The VSA report must contain:

(i) A summary of how the on-scene survey was conducted;

(ii) Existing security measures, procedures, and operations;

(iii) A description of each vulnerability found during the assessment;

(iv) A description of security countermeasures that could be used to address each vulnerability;

(v) A list of the key vessel operations that are important to protect;

(vi) The likelihood of possible threats to key vessel operations; and

(vii) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the vessel.

(2) The VSA report must address the following elements on board or within the vessel:

(i) Physical security;

(ii) Structural integrity;

(iii) Personnel protection systems;

(iv) Procedural policies;

(v) Radio and telecommunication systems, including computer systems and networks; and

(vi) Other areas that may, if damaged or used illicitly, pose a risk to people, property, or operations on board the vessel or within a facility.

(3) The VSA must list the persons, activities, services, and operations that are important to protect, in each of the following categories:

(i) Vessel personnel;

(ii) Passengers, visitors, vendors, repair technicians, facility personnel, etc.;

(iii) Capacity to maintain safe navigation and emergency response;

(iv) Cargo, particularly dangerous goods or hazardous substances;

(v) Vessel stores;

(vi) Any vessel security communication and surveillance systems; and

(vii) Any other vessel security systems, if any.

(4) The VSA must account for any vulnerabilities in the following areas:

(i) Conflicts between safety and security measures;

(ii) Conflicts between vessel duties and security assignments;

(iii) The impact of watch-keeping duties and risk of fatigue on vessel personnel alertness and performance;

(iv) Security training deficiencies; and

(v) Security equipment and systems, including communication systems.

(5) The VSA must discuss and evaluate key vessel measures and operations, including:

(i) Ensuring performance of all security duties;

(ii) Controlling access to the vessel, through the use of identification systems or otherwise;

(iii) Controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied);

(iv) Supervising the handling of cargo and the delivery of vessel stores;

(v) Monitoring restricted areas to ensure that only authorized persons have access;

(vi) Monitoring deck areas and areas surrounding the vessel; and

(vii) The ready availability of security communications, information, and equipment.

(6) The VSA must be documented and the VSA report retained by the vessel owner or operator with the VSP. The VSA and VSP must be protected from unauthorized access or disclosure.

§§ 104.310 Submission requirements.

(a) A completed Vessel Security Assessment (VSA) report must be submitted with the Vessel Security Plan (VSP) required in § 104.410 of this part.

(b) A vessel owner or operator may generate and submit a report that contains the VSA for more than one vessel subject to this part, to the extent that they share similarities in physical characteristics and operations.

Subpart D—Vessel Security Plan (VSP)

§ 104.400 General.

(a) The Company Security Officer (CSO) must ensure a Vessel Security Plan (VSP) is developed and implemented for each vessel. The VSP:

(1) Must identify the CSO and VSO by name or position and provide 24-hour contact information;

(2) Must be written in English;

(3) Must address each vulnerability identified in the Vessel Security Assessment (VSA);

(4) Must describe security measures for each MARSEC Level;

(5) Must state the Master's authority as described in § 104.205; and

(6) May cover more than one vessel to the extent that they share similarities in physical characteristics and operations, if authorized and approved by the Commanding Officer, Marine Safety Center.

(b) Except for foreign vessels that have on board a valid International Ship Security Certificate (ISSC) that attests to the vessel's compliance with SOLAS Chapter XI–2 and the ISPS Code, part A (Incorporated by reference, see § 101.115 of this subchapter), and having taken into account the relevant provisions in the ISPS Code, part B, the VSP must be submitted for approval to the Commanding Officer, Marine Safety Center (MSC), 400 Seventh Street, SW., Room 6302, Nassif Building, Washington, DC 20590–0001, in a written or electronic format. Format for submitting the VSP electronically can be found at *http://www.uscg.mil/HQ/MSC*.

(c) The VSP is sensitive security information and must be protected in accordance with 49 CFR part 1520.

(d) If the VSP is kept in an electronic format, procedures must be in place to prevent its unauthorized deletion, destruction, or amendment.